Alert (TA16-288A)

Heightened DDoS Threat Posed by Mirai and Other Botnets

Original release date: October 14, 2016 | Last revised: October 17, 2016

Systems Affected

Internet of Things (IoT)—an emerging network of devices (e.g., printers, routers, video cameras, smart TVs) that connect to one another via the Internet, often automatically sending and receiving data

Overview

Recently, IoT devices have been used to create large-scale botnets—networks of devices infected with self-propagating malware—that can execute crippling distributed denial-of-service (DDoS) attacks. IoT devices are particularly susceptible to malware, so protecting these devices and connected hardware is critical to protect systems and networks.

Description

On September 20, 2016, Brian Krebs' security blog (krebsonsecurity.com) was targeted by a massive DDoS attack, one of the largest on record, exceeding 620 gigabits per second (Gbps).[1] An IoT botnet powered by Mirai malware created the DDoS attack. The Mirai malware continuously scans the Internet for vulnerable IoT devices, which are then infected and used in botnet attacks. The Mirai bot uses a short list of 62 common default usernames and passwords to scan for vulnerable devices. Because many IoT devices are unsecured or weakly secured, this short dictionary allows the bot to access hundreds of thousands of devices.[2] The purported Mirai author claimed that over 380,000 IoT devices were enslaved by the Mirai malware in the attack on Krebs' website.[3]

In late September, a separate Mirai attack on French webhost OVH broke the record for largest recorded DDoS attack. That DDoS was at least 1.1 terabits per second (Tbps), and may have been as large as 1.5 Tbps.[4]

The IoT devices affected in the latest Mirai incidents were primarily home routers, network-enabled cameras, and digital video recorders.[5] Mirai malware source code was published online at the end of September, opening the door to more widespread use of the code to create other DDoS attacks.

In early October, Krebs on Security reported on a separate malware family responsible for other IoT botnet attacks.[6] This other malware, whose source code is not yet public, is named Bashlite. This malware also infects systems through default usernames and passwords. Level 3 Communications, a security firm, indicated that the Bashlite botnet may have about one million enslaved IoT devices.[7]

Impact

With the release of the Mirai source code on the Internet, there are increased risks of more botnets being generated. Both Mirai and Bashlite can exploit the numerous IoT devices that still use default passwords and are easily compromised. Such botnet attacks could severely disrupt an organization's communications or cause significant financial harm.

Software that is not designed to be secure contains vulnerabilities that can be exploited. Software-connected devices collect data and credentials that could then be sent to an adversary's collection point in a back-end application.

Solution

Cybersecurity professionals should harden networks against the possibility of a DDoS attack. For more information on DDoS attacks, please refer to US-CERT Security Publication DDoS Quick Guide and the US-CERT Alert on UDP-Based Amplification Attacks.

Mitigation

In order to remove the Mirai malware from an infected IoT device, users and administrators should take the following actions:

- Disconnect device from the network.
- While disconnected from the network and Internet, perform a reboot. Because Mirai malware exists in dynamic memory, rebooting the device clears the malware [8].
- Ensure that the password for accessing the device has been changed from the default password to a strong password. See US-CERT Tip Choosing and Protecting Passwords for more information.
- You should reconnect to the network only after rebooting and changing the password. If you reconnect before changing the password, the device could be quickly reinfected with the Mirai malware.

Preventive Steps

In order to prevent a malware infection on an IoT device, users and administrators should take following precautions:

- Ensure all default passwords are changed to strong passwords. Default usernames and passwords for most devices can easily be found on the Internet, making devices with default passwords extremely vulnerable.
- Update IoT devices with security patches as soon as patches become available.
- Disable Universal Plug and Play (UPnP) on routers unless absolutely necessary.[9]
- Purchase IoT devices from companies with a reputation for providing secure devices.
- Consumers should be aware of the capabilities of the devices and appliances installed in their homes and businesses. If a device comes with a default password or an open Wi-Fi connection, consumers should change the password and only allow it to operate on a home network with a secured Wi-Fi router.
- Understand the capabilities of any medical devices intended for at-home use. If the device transmits data or can be operated remotely, it has the potential to be infected.
- Monitor Internet Protocol (IP) port 2323/TCP and port 23/TCP for attempts to gain unauthorized control over IoT devices using the network terminal (Telnet) protocol.[10]

- Look for suspicious traffic on port 48101. Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor.

References

- [1] KrebsOnSecurity: KrebsOnSecurity Hit With Record DDoS
- [2] Sophos: Mirai “internet of things” malware from Krebs DDoS attack goes open source
- [3] PCWorld: Smart device malware behind record DDoS attack is now available to all hackers
- [4] ArsTechnica: Record-breaking DDoS reportedly delivered by >145k hacked cameras
- [5] InformationWeek DarkReading: IoT DDoS Attack Code Released
- [6] KrebsOnSecurity: Source Code for IoT Botnet "Mirai" Released
- [7] Level 3 Threat Research Labs: Attack of Things!
- [8] ICS-CERT: Sierra Wireless Mitigations Against Mirai Malware
- [9] Federal Bureau of Investigation Public Service Announcement: Internet of Things Poses Opportunities for Cyber Crime
- [10] SANS ISC InfoSec Forums: What is happening on 2323/TCP?

Revisions

- October 14, 2016: Initial release
- October 17, 2016: Added ICS-CERT reference [8]